

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-224189

(43)Date of publication of application : 17.08.1999

(51)Int.Cl. G06F 9/06  
 G06F 12/14  
 G09C 1/00  
 H04L 9/32

(21)Application number : 10-041253

(71)Applicant : NIPPON CHEMICON CORP

(22)Date of filing : 06.02.1998

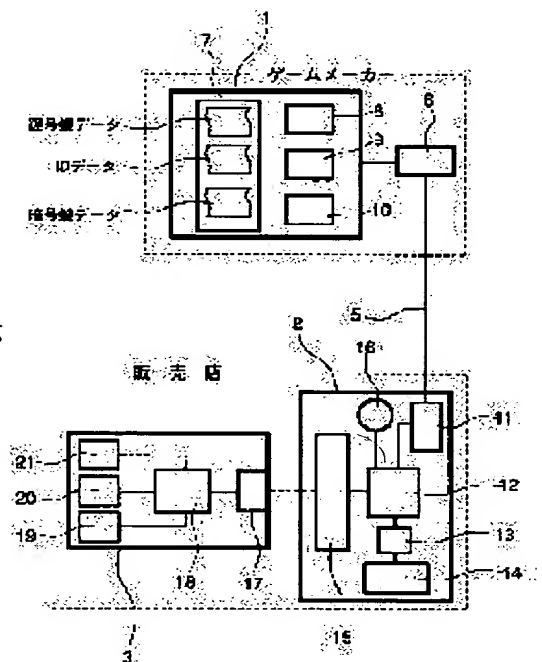
(72)Inventor : YAMAMOTO KAZUYUKI

## (54) DECODING KEY DATA WRITING SYSTEM

## (57)Abstract:

**PROBLEM TO BE SOLVED:** To provide a decoding key data writing system by which decoding key data are not appropriated by a third person even at the time of distribution or writing in an IC card.

**SOLUTION:** This system consists of a host computer 1 provided with a storage device 7 for storing decoding key data for decoding ciphered program data, identifying data intrinsically imparted to the IC card and cipher key data corresponding to the identifying data and with a cipher generating device 8 for enciphering decoding key data, the IC card 3 provided with a memory part 19 for storing decoding key data, identifying data and cipher key data corresponding to identifying data, with a cipher processing part 21 for restoring enciphered decoding key data and with a control part 18, an IC card reader/ writer 2 and a communication means 5 connecting the host computer to the IC card reader/writer 2. Enciphered decoding key data are written in the IC card by cipher key data corresponding to identifying data.



## LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平11-224189

(43) 公開日 平成11年(1999) 8月17日

(51) Int.Cl.<sup>6</sup>

識別記号

F I

G 0 6 F 9/06

5 5 0

G 0 6 F 9/06

5 5 0 C

12/14

3 2 0

12/14

3 2 0 B

G 0 9 C 1/00

6 6 0

G 0 9 C 1/00

6 6 0 A

H 0 4 L 9/32

H 0 4 L 9/00

6 7 3 C

審査請求 未請求 請求項の数 4 F D (全 9 頁)

(21) 出願番号 特願平10-41253

(22) 出願日 平成10年(1998) 2月6日

(71) 出願人 000228578

日本ケミコン株式会社

東京都青梅市東青梅1丁目167番地の1

(72) 発明者 山本 和行

東京都青梅市東青梅1丁目167番地の1

日本ケミコン株式会社内

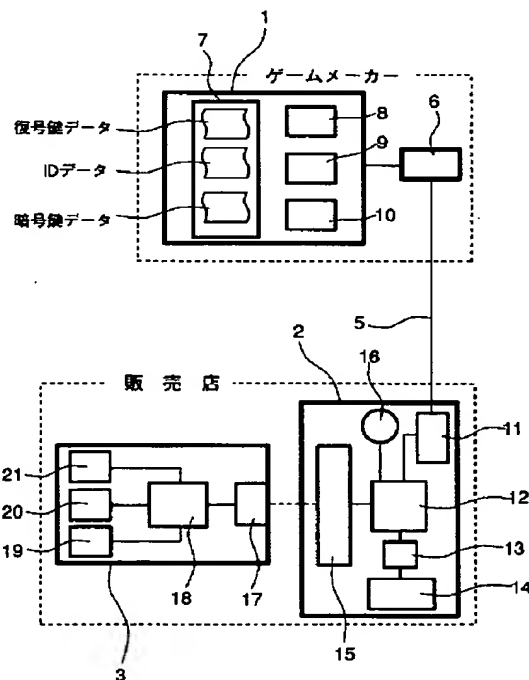
(74) 代理人 弁理士 日高 一樹 (外1名)

(54) 【発明の名称】 復号鍵データの書き込みシステム

(57) 【要約】

【課題】 配信時やICカードへの書き込み時においても第三者によって、復号鍵データが盗用されることのない復号鍵データの書き込みシステムを提供する。

【解決手段】 暗号化されているプログラムデータを復号する復号鍵データとICカードに固有に付与された識別データとこの識別データと対応付けられた暗号鍵データとを記憶する記憶装置7と、前記復号鍵データを暗号化する暗号生成装置8とを具備するホストコンピュータ1と、前記復号鍵データおよび前記識別データおよび識別データと対応付けられた暗号鍵データとを記憶するメモリ部19と、前記暗号化された復号鍵データを復元する暗号処理部21と、制御部18とを具備するICカード3と、ICカードリーダーライタ2と、前記ホストコンピュータ1とICカードリーダーライタ2とを接続する通信手段5と、から成り、前記識別データに対応付けられた暗号鍵データにより、暗号化された復号鍵データがICカード3に書き込まれるようにする。



## 【特許請求の範囲】

【請求項1】 光記憶ディスク等の記憶媒体に暗号化されて記憶されているプログラムデータを復号する復号鍵データとICカードに固有に付与されたID等の識別データとこの識別データと対応付けられた暗号鍵データとを記憶する記憶装置と、前記暗号鍵データにより所定のアルゴリズムに基づいて前記復号鍵データを暗号化する暗号生成装置とを具備するホストコンピュータと、前記復号鍵データおよびICカードに固有に付与されたID等の識別データとこの識別データと対応付けられた暗号鍵データとを記憶する不揮発性のメモリ部と、前記ホストコンピュータより出力される暗号化された復号鍵データを前記メモリ部に記憶されている暗号鍵データによって復元する暗号処理部と、これら各部を制御する制御部とを具備するICカードと、このICカードに書き込み、読み出しを行うICカードリーダライタと、前記ホストコンピュータとICカードリーダライタとを接続する通信手段と、から成り、前記暗号化された復号鍵データがホストコンピュータよりICカードに書き込まれる際に、前記ID等の識別データがICカードより読み出され、そのID等の識別データに対応付けられてホストコンピュータの記憶装置に記憶されている暗号鍵データにより、暗号生成装置にて暗号化された復号鍵データが、通信手段およびICカードリーダライタを介してICカードに出力されることを特徴とする復号鍵データの書き込みシステム。

【請求項2】 前記復号鍵データが、ICカードにおいて前記暗号化された状態の復号鍵データとして記憶されており、必要に応じて復号鍵データに復元されるようになっている請求項1に記載の復号鍵データの書き込みシステム。

【請求項3】 前記ICカードのメモリ部に記憶された暗号鍵データが、ICカードより読み出し不可とされている請求項1または2に記載の復号鍵データの書き込みシステム。

【請求項4】 所定長のランダムデータを生成するランダムデータ生成手段と、前記メモリ部に記憶されている暗号鍵データにより暗号化されたランダムデータを復元する復元手段と、この復元されたランダムデータと前記ランダムデータ生成手段により生成された所定長のランダムデータとを比較する比較手段とが前記ホストコンピュータに設けられるとともに、前記所定長のランダムデータを前記メモリ部に記憶された暗号鍵データにより暗号化する暗号生成部が前記ICカードに設けられ、暗号化された復号鍵データがICカードに出力される際に、前記所定長のランダムデータがホストコンピュータからICカードに出力され、ICカードにおいてこのランダムデータが、前記暗号生成部により暗号化され、この暗号化されたランダムデータがホストコンピュータに返

送、前記復元手段により復元されるとともに、前記比較手段によって元のランダムデータと比較され、これらが一致した場合に暗号化された復号鍵データがホストコンピュータより出力されるようになっている請求項1～3のいずれかに記載の復号鍵データの書き込みシステム。

## 【発明の詳細な説明】

## 【0001】

【発明の属する技術の分野】 本発明は、CDROMやDVD等の記憶媒体に暗号化されて記憶されているゲームソフト等のプログラムデータを復号する復号鍵データ（ライセンス鍵データ）の盗用を防止することのできる復号鍵データの書き込みシステムに関する。

## 【0002】

【従来の技術】 近年、CDROMやDVD等の記憶媒体に記憶されたゲームソフト等のプログラムデータを不正にコピーして使用する不正使用が社会的な問題となっている。

【0003】 これら不正使用を防止するための方法として、これら光記憶媒体であるCDROMやDVD等に記憶されるプログラムデータを暗号鍵データ等により暗号化して記憶しておき、これら暗号化されたプログラムデータを復号する復号鍵データ（ライセンス鍵データ）を入手しないと、暗号化されたプログラムデータを平文データに復号することができないようにして、不正なコピーや使用を防止する方法が提案されている。

【0004】 しかしながら、これら復号鍵データ（ライセンス鍵データ）を用いた場合においては、暗号化されたプログラムデータそのものを複製しても、そのまま使用することができないようにすることはできるものの、この復号鍵データ（ライセンス鍵データ）が第三者によって盗用、入手されると、容易に不正な使用が可能になってしまうという問題点があるため、これら復号鍵データ（ライセンス鍵データ）を盗用されないように、ユーザーに配布する必要があった。

【0005】 これら盗用の問題を解決するために、近年ではこれら復号鍵データ（ライセンス鍵データ）をICカード等の電子記憶媒体に記憶して、各ユーザーにライセンスカードとして配布し、ユーザーにおいても復号鍵データ（ライセンス鍵データ）が不明なようにして、そのICカードがないとプログラムデータを使用できないようにする試みがなされている。

## 【0006】

【発明が解決しようとする課題】 しかしながら、これらICカードを用いた復号鍵データ（ライセンス鍵データ）の配布方法は、復号鍵データ（ライセンス鍵データ）の盗用を一元的には防止できるものの、通常においてこれらライセンスカードは、各販売店等にて、前記ICカードに復号鍵データ（ライセンス鍵データ）が書き込まれているため、これら各販売店等に復号鍵データ（ライセンス鍵データ）を配信しICカードへ書き込む

際において、復号鍵データ（ライセンス鍵データ）が盗用される可能性が高いという問題があった。

【0007】よって、本発明は上記した問題点に着目してなされたもので、各販売店等への配信時やＩＣカードへの書き込み時においても第三者によって、復号鍵データ（ライセンス鍵データ）が盗用されることのない復号鍵データの書き込みシステムを提供することを目的としている。

【0008】

【課題を解決するための手段】前記した問題を解決するために、本発明の復号鍵データの書き込みシステムは、光記憶ディスク等の記憶媒体に暗号化されて記憶されているプログラムデータを復号する復号鍵データとＩＣカードに固有に付与されたＩＤ等の識別データとこの識別データと対応付けられた暗号鍵データとを記憶する記憶装置と、前記暗号鍵データにより所定のアルゴリズムに基づいて前記復号鍵データを暗号化する暗号生成装置とを具備するホストコンピュータと、前記復号鍵データおよびＩＣカードに固有に付与されたＩＤ等の識別データとこの識別データと対応付けられた暗号鍵データとを記憶する不揮発性のメモリ部と、前記ホストコンピュータより出力される暗号化された復号鍵データを前記メモリ部に記憶されている暗号鍵データによって復元する暗号処理部と、これら各部を制御する制御部とを具備するＩＣカードと、このＩＣカードに書き込み、読み出しを行うＩＣカードリーダライタと、前記ホストコンピュータとＩＣカードリーダライタとを接続する通信手段と、から成り、前記暗号化された復号鍵データがホストコンピュータよりＩＣカードに書き込まれる際に、前記ＩＤ等の識別データがＩＣカードより読み出され、そのＩＤ等の識別データに対応付けられてホストコンピュータの記憶装置に記憶されている暗号鍵データにより、暗号生成装置にて暗号化された復号鍵データが、通信手段およびＩＣカードリーダライタを介してＩＣカードに出力されることを特徴としている。この特徴によれば、ホストコンピュータより販売店およびＩＣカードに復号鍵データが配信、書き込まれる際に、ホストコンピュータより出力される復号鍵データが、ＩＣカードに個別に付与されたＩＤ等の識別データと関連付けられた暗号鍵データにより暗号化されて出力されるため、第三者により復号鍵データ自体が盗用されることなく、復号鍵データを販売店およびＩＣカードに配信、書き込むことができる。

【0009】本発明の復号鍵データの書き込みシステムは、前記復号鍵データが、ＩＣカードにおいて前記暗号化された状態の復号鍵データとして記憶されており、必要に応じて復号鍵データに復元されるようになっていることが好ましい。このようにすれば、ＩＣカード内部において、復号鍵データが暗号化された状態にて記憶されているため、第三者によって復号鍵データ自体をＩＣカード内部より読み出されて盗用されることを防ぐことが

できる。

【0010】本発明の復号鍵データの書き込みシステムは、前記ＩＣカードのメモリ部に記憶された暗号鍵データが、ＩＣカードより読み出し不可とされていることが好ましい。このようにすれば、仮にＩＣカードより暗号化された復号鍵データが盗用されたとしても、第三者によってＩＣカードより暗号鍵データが読み出されて、前記暗号化された復号鍵データが復元されることを防止できる。

【0011】本発明の復号鍵データの書き込みシステムは、所定長のランダムデータを生成するランダムデータ生成手段と、前記メモリ部に記憶されている暗号鍵データにより暗号化されたランダムデータを復元する復元手段と、この復元されたランダムデータと前記ランダムデータ生成手段により生成された所定長のランダムデータとを比較する比較手段とが前記ホストコンピュータに設けられるとともに、前記所定長のランダムデータを前記メモリ部に記憶された暗号鍵データにより暗号化する暗号生成部が前記ＩＣカードに設けられ、暗号化された復号鍵データがＩＣカードに出力される際に、前記所定長のランダムデータがホストコンピュータからＩＣカードに出力され、ＩＣカードにおいてこのランダムデータが、前記暗号生成部により暗号化され、この暗号化されたランダムデータがホストコンピュータに返送、前記復元手段により復元されるとともに、前記比較手段によって元のランダムデータと比較され、これらが一致した場合に暗号化された復号鍵データがホストコンピュータより出力されるようになっていることが好ましい。このようにすれば、書き込みがなされるＩＣカードが正規のＩＣカードであるか否かを暗号化された復号鍵データを出力する以前にホストコンピュータが確認できるばかりか、ホストコンピュータに識別データと関連付けて記憶されている復号鍵データに誤りがないか否かを確認することもできる。

【0012】

【発明の実施の形態】以下、図面に基づいて本発明の実施形態を説明する。

【0013】図１は、本実施例における復号鍵データの書き込みシステムを用いたライセンスカードシステムを示す図であり、図２は本実施例における復号鍵データの書き込みシステムの各構成を示すブロック図であり、図３は、本実施例におけるホストコンピュータに用いた暗号生成装置での処理内容を示す図であり、図４は、本実施例におけるＩＣカードに用いた暗号処理部での処理内容を示す図であり、図５は、本実施例において用いた暗号処理アルゴリズムの処理概要を示す図であり、図６は、ホストコンピュータとＩＣカード発行装置とＩＣカードとの処理動作を示す図である。

【0014】本実施例では、本発明の復号鍵データの書き込みシステムをゲームプログラムのライセンスカード

システムに応用したものである。

【0015】本実施例のゲームプログラムのライセンスカードシステムは、図1に示されるような構成とされており、ゲームメーカーに配置されたホストコンピュータ1と、各販売店に設置されたICカード発行装置2と、ライセンス鍵である復号鍵データが書き込み、記憶されるICカード3と、このICカード3を装着可能とされたゲームプログラムの再生装置4と、暗号化されたゲームプログラムデータが記憶され、この再生装置4にて再生されるCDROMと、から主に構成されており、前記の暗号化されたゲームプログラムデータが記憶されたCDROMは、ゲームメーカーより各ユーザーに配付され、各販売店にてそのCDROMに対応する前記復号鍵データが、前記ICカード3に書き込むことにより販売され、各ユーザーがそのICカード3を再生装置4に装着することにより、ICカード3に記憶されている復号鍵データが読み出されて、CDROMに記憶されている暗号化されたゲームプログラムデータが復号されて実行可能なようになっている。

【0016】前記ライセンスカードシステムに用いた本実施例の復号鍵データの書き込みシステムは、図2に示されるような構成とされており、前記ホストコンピュータ1は、その特徴として、ハードディスク等の記憶装置7内部に、ライセンス鍵である復号鍵データ(PT)と、データベース化された各ICカード3に固有に付与されているIDデータおよび各IDデータと1対1に対応付けられた暗号鍵データ(KA)とが記憶されており、さらにこの復号鍵データ(PT)を前記暗号鍵データ(KA)により暗号化するとともに、ICカード3より返送されてくる暗号化されたランダムデータ(AR)を復元する暗号生成装置8と、所定長のランダムデータ(TR)を生成するランダムデータ生成装置9と、これらランダムデータ(TR)と前記ICカード3より返送され暗号生成装置8によって復元された復元ランダムデータ(FR)とを比較する比較部10が設けられており、このホストコンピュータ1は、通信モデム6および通信回線5を介して前記ICカード発行装置2と接続されている。

【0017】この各販売店に設置されたICカード発行装置2は、図2に示されるような構成とされており、前記通信モデム6とのデータ通信を実施する通信モデム部11と、ICカード3が挿入されることによりICカード3とのデータのやり取りを実施するICカードリーダライタ部15と、表示部としてのLCDパネル14と、このLCDパネル14の表示動作を制御するLCDドライバ13と、発行スイッチ16と、これら各部の制御を実施するマイクロプロセッシングユニット(MPU)12が設けられ、このMPU12の内部には内部ROM(図示せず)が設けられ、MPU12が行う制御動作が記述されたプログラムが予め記憶、格納されている。

【0018】また、前記ICカード3の構成は、図2に示されるようになっており、本実施例では、各ICカード3には固有のIDが付与されており、これらIDデータおよびこのIDデータと1対1に対応付けられた暗号鍵データ(KB)並びに前記ホストコンピュータ1より出力される暗号化された復号鍵データ(PA)とを記憶する不揮発性メモリであるEEPROM部19と、各種演算等において使用されるメモリ部20と、後述する所定のアルゴリズムに基づき、前記EEPROM部19に記憶されている暗号鍵データ(KB)により、ホストコンピュータ1より出力される所定長のランダムデータ

(TR)の暗号化および前記暗号化された復号鍵データ(PA)の復元を実施する暗号処理部21と、前記ICカードリーダライタ部15とのデータのやり取りを実施する通信部17と、これら各部の制御等を実施する制御部18とが設けられており、前記EEPROM部19にはICカード3に付与された前記IDデータおよび暗号鍵データ(KB)が予め記憶されており、この暗号鍵データ(KB)は、図5に示されるように、前記ホストコンピュータ1に記憶されている暗号鍵データ(KA)と所定の規則に基づいて双方の暗号鍵データで暗号化されたデータを復元可能な鍵データ組として1セットとされており、ICカード3外部よりその出力が指示されても、暗号鍵データ(KA)が出力されないように、前記EEPROM部19の特定のアドレスに記憶されるようになっており、このアドレスの読み出し指示は、前記暗号処理部21からの出力のみが有効となるように制御部18にプログラムされている。

【0019】本実施例において、前記ホストコンピュータ1内部に設けられた暗号生成装置8での暗号化処理の内容は、図3に示されるようになっており、書き込みがなされるICカード3のIDに対応する暗号鍵データ(KA)が入力されることにより、この暗号鍵データ(KA)に基づき、入力された復号鍵データ(PT)をべき乗剰余演算アルゴリズムにより演算処理し、同一桁数の配列が異なる暗号化された復号鍵データ(PA)とするとともに、前記ICカード3より送られてきた、暗号鍵データ(KB)に基づき暗号化された暗号化ランダムデータ(AR)を、上記の復号鍵データ(PT)の暗号化処理同様に、暗号鍵データ(KA)に基づき、べき乗剰余演算アルゴリズムにより演算処理することにより、復元ランダムデータ(FR)に復元されるようになっている。

【0020】また、ICカード3内部に設けられた前記暗号処理部21の処理内容は、図4に示されるようになっており、予め前記EEPROM部19に記憶されている暗号鍵データ(KB)が入力されることにより、この暗号鍵データ(KB)に基づき、ホストコンピュータ1より出力される所定長のランダムデータ(TR)をべき乗剰余演算アルゴリズムにより演算処理し、同一桁数の

配列が異なる暗号化ランダムデータ (AR) とするとともに、前記ホストコンピュータ 1 にて暗号鍵データ (KA) により暗号化された復号鍵データ (PA) を、べき乗剰余演算アルゴリズムにより演算処理し、復号鍵データ (PT) に復元するようになっている。

【0021】これら本実施例において用いた、前記べき乗剰余演算アルゴリズムの処理内容は、図 5 に示されるようになっており、暗号化処理においては、図 5 (a) に示すように、入力されたデータ列の各桁の数値を、所定の暗号鍵データ (KA) により乗数計算し、その計算値の所定の桁 (本実施例では最小桁) の数値を出力データとして暗号化を実施するようになっており、これら暗号化されたデータ列の復元を実施する復元処理においては、図 5 (b) に示すように、前記暗号化に用いた暗号鍵データと対をなす所定の暗号鍵データ (KB) により、暗号化と同様の処理を実施することにより、元のデータ列が復元されるようになっている。

【0022】これらホストコンピュータ 1 と IC カード発行装置 2 と IC カード 3 との間におけるデータ等のやり取りおよびその処理内容は、図 6 に示されるようになっており、IC カード 3 が IC カード発行装置 2 の IC カードリーダー 8 に挿入されると、IC カード 3 の挿入が検出され、IC カード 3 に対して予め EEPROM 部 19 に記憶されている ID データを出力するように、IC カード発行装置 2 の MPU 12 が指示を出力する。

【0023】この出力に基づいて、IC カード 3 に内蔵されている制御部 18 は、ID データを EEPROM 部 19 より読み出し、通信部 17 を介して IC カード発行装置 2 に出力し、この ID データが通信回線 5 を介してホストコンピュータ 1 に伝送される。

【0024】この ID データの出力により、ホストコンピュータ 1 は、記憶装置 7 内部に記憶されているデータベースから、この ID データに対応付けられて記憶されている暗号鍵データ (KA) を検索するとともに、前記ランダムデータ生成装置 9 にて所定長のランダムデータ (TR) を生成し、このランダムデータ (TR) を IC カード発行装置 2 を介して IC カード 3 に出力する。

【0025】次いで IC カード 3 では、このランダムデータ (TR) を前記暗号処理部 21 にて、予め EEPROM 部 19 に記憶されている暗号鍵データ (KB) によって暗号化を実施し、この暗号化されたランダムデータ (AR) を IC カード発行装置 2 を介してホストコンピュータ 1 に返送する。

【0026】ホストコンピュータ 1 では、この返送されてきた暗号化されたランダムデータ (AR) を、前記暗号生成装置 8 にて、前記検索された暗号鍵データ (KA) に基づき復元を実施して復元ランダムデータ (FR) とし、これら復元ランダムデータ (FR) と前記ランダムデータ (TR) とが一致するかを比較部において比較し、IC カードが正規のものであるか否かの認証を

実施し、その認証結果を IC カード発行装置 2 に出力する。

【0027】この認証結果の出力に基づき、IC カード発行装置 2 は、その認証結果が「否」である場合には、認証のエラーを前記 LCD パネル 14 に表示し、IC カード 3 を排出して処理を終了し、その認証結果が「可」である場合には、LCD パネル 14 に「発行スイッチを押して下さい」のメッセージを表示し、発行スイッチ 5 の入力待ちを所定時間行い、所定時間内に発行スイッチ 5 が入力されない場合には、IC カード 3 を排出して、処理を終了する。

【0028】発行スイッチ 5 が所定時間内に入力され場合には、IC カード発行装置 2 は、ホストコンピュータ 1 に対して暗号化された復号鍵データ (PA) の出力を指示する。

【0029】ホストコンピュータ 1 は、この指示により前記記憶装置 7 内部に記憶されている復号鍵データ (PT) を、前記検索された暗号鍵データ (KA) によって前記暗号生成装置 8 にて暗号化を実施し、暗号化された復号鍵データ (PA) を生成させ、これを IC カード発行装置 2 を介して IC カード 3 に出力する。

【0030】この暗号化された復号鍵データ (PA) は、IC カード 3 において、暗号化されたままの状態にて前記 EEPROM 部 19 に書き込み、記憶され、IC カード 3 の制御部 18 は、前記書き込みが終了すると書き込み完了を IC カード発行装置 2 に出力し、この出力に基づき、IC カード発行装置 2 から IC カード 3 が排出されて、処理が終了する。

【0031】このようにして前記 EEPROM 部 19 に記憶された暗号化された状態の復号鍵データ (PA) は、EEPROM 部 19 に予め記憶されている暗号鍵データ (KB) により、必要に応じて前記暗号処理部 21 にて復元されて使用されるようになっている。

【0032】以上、本発明を図面に基づいて説明してきたが、本発明は前記実施例に限定されるものではなく、本発明の主旨を逸脱しない範囲での変更や追加があっても、本発明に含まれることは言うまでもない。

【0033】また、前記実施例では、ゲームプログラムのライセンスカードシステムを例として説明しているが、本発明はゲームプログラム以外のその他のプログラムデータ等においても同様の効果が得られることは言うまでもなく、それらプログラムデータが記憶される記憶媒体も、本実施例では CDROM が使用されているが、これに限定されるものではなく、その他の記憶媒体であっても良い。

【0034】また、本実施例では、前記ホストコンピュータ 1 に記憶されている暗号鍵データ (KA) と IC カード 3 に予め記憶されている暗号鍵データ (KB) とが、相関する 1 セットの組を形成しているものの、異なるデータとされているが、本発明はこれに限定されるも

10

20

30

40

50

のではなく、適宜な暗号化アルゴリズムを用いて、これら暗号鍵データを同一のものとするようにしても良い。

【0035】また、本実施例では、復号鍵データを固定としているが、これら復号鍵データを、プログラムデータ毎に個別のものとしても良く、この場合においては、そのプログラムに対応する復号鍵データを特定するために、ホストコンピュータ 1 に IC カード発行装置 2 等からプログラムを特定可能とする情報、例えばプログラムナンバーや種別等を示す略号等を出力するようにして、そのプログラムだけを復号可能とするようにしても良い。

【0036】また、前記 IC カード 3 をユーザー毎に個別のものとしておき、IC カード 3 の前記 EEPROM 部 1 9 に、ユーザー情報等を記憶しておき、復号鍵データを書き込む際に、これらユーザー情報をホストコンピュータ 1 に出力させて、顧客管理が可能ないようにしても良い。

【0037】また、本実施例においては、前記 IC カード 3 の不揮発性メモリとして EEPROM を使用しているが、本発明はこれに限定されるものではなく、その他の不揮発性メモリ、例えば誘電体メモリ (FeRAM) やフラッシュメモリ等を使用しても良い。

【0038】

【発明の効果】本発明は次の効果を奏する。

【0039】(a) 請求項 1 の発明によれば、ホストコンピュータより販売店および IC カードに復号鍵データが配信、書き込まれる際に、ホストコンピュータより出力される復号鍵データが、IC カードに個別に付与された ID 等の識別データと関連付けられた暗号鍵データにより暗号化されて出力されるため、第三者により復号鍵データ自体が盗用されることなく、復号鍵データを販売店および IC カードに配信、書き込むことができる。

【0040】(b) 請求項 2 の発明によれば、IC カード内部において、復号鍵データが暗号化された状態にて記憶されているため、第三者によって復号鍵データ自体を IC カード内部より読み出されて盗用されることを防ぐことができる。

【0041】(c) 請求項 3 の発明によれば、仮に IC カードより暗号化された復号鍵データが盗用されたとしても、第三者によって IC カードより暗号鍵データが読み出されて、前記暗号化された復号鍵データが復元されることを防止できる。

【0042】(d) 請求項 4 の発明によれば、書き込み

がなされる IC カードが正規の IC カードであるか否かを暗号化された復号鍵データを出力する以前にホストコンピュータが確認できるばかりか、ホストコンピュータに識別データと関連付けて記憶されている復号鍵データに誤りが無いか否かを確認することもできる。

【0043】

【図面の簡単な説明】

【図 1】本発明の実施例における復号鍵データの書き込みシステムを用いたライセンスカードシステムを示す図である。

【図 2】本発明の実施例における復号鍵データの書き込みシステムの各構成を示すブロック図である。

【図 3】本発明の実施例におけるホストコンピュータに用いた暗号生成装置での処理内容を示す図である。

【図 4】本発明の実施例における IC カードに用いた暗号処理部での処理内容を示す図である。

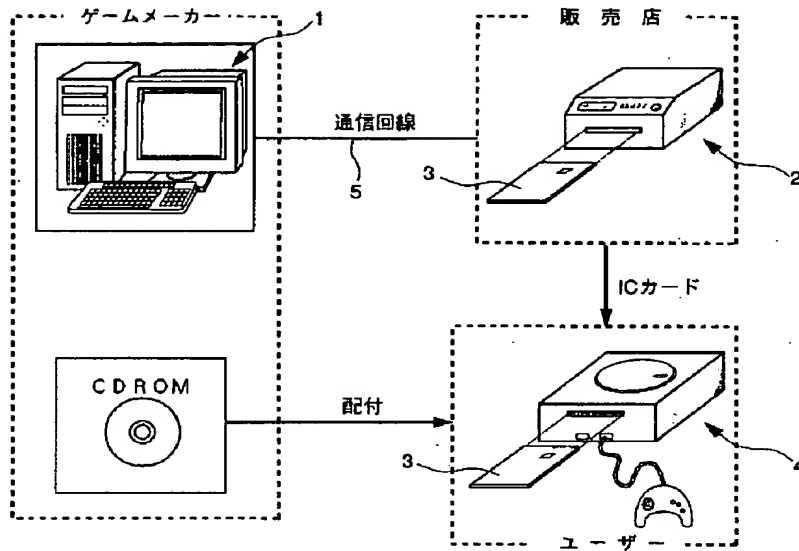
【図 5】(a)、(b) 本発明の実施例に用いたべき乗剰余演算アルゴリズムの処理概要を示す図である。

【図 6】本発明の実施例におけるホストコンピュータと IC カード発行装置と IC カードとの処理動作を示す図である。

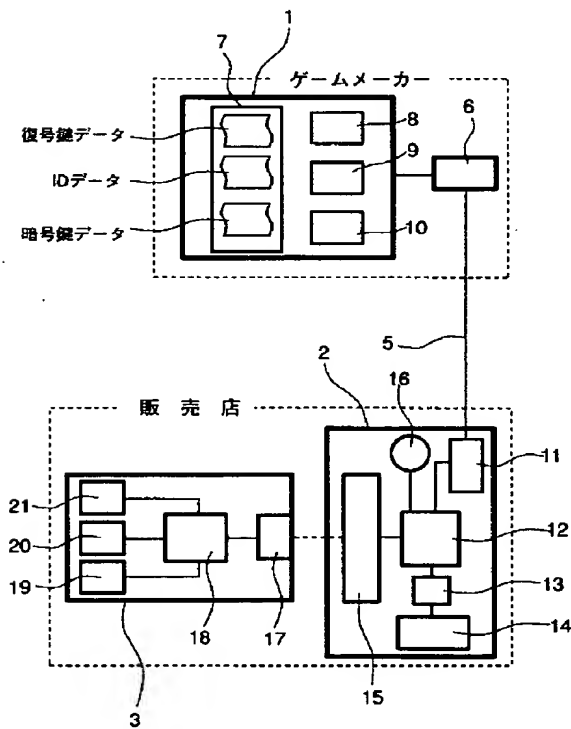
【符号の説明】

1	ホストコンピュータ
2	IC カード発行装置
3	IC カード
4	再生装置
5	通信回線 (通信手段)
6	通信モデム (通信手段)
7	記憶装置
8	暗号生成装置
9	ランダムデータ生成装置
10	比較部 (比較手段)
11	通信モデム部 (通信手段)
12	マイクロプロセッシングユニット (MPU)
13	LCD ドライバ
14	LCD パネル
15	IC カードリーダーライタ部
16	発行スイッチ
17	通信部
18	制御部
19	EEPROM 部 (不揮発性メモリ部)
20	メモリ部
21	暗号処理部

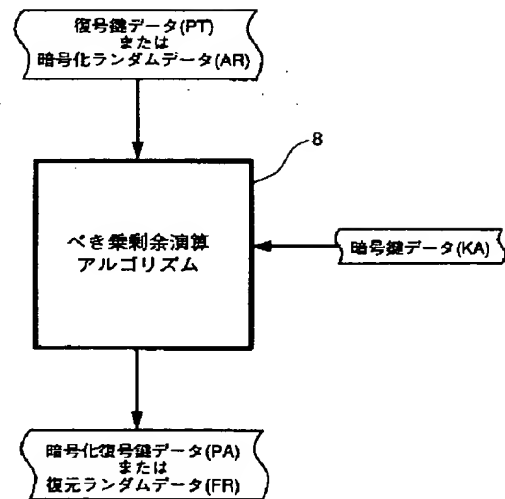
【図1】



【図2】

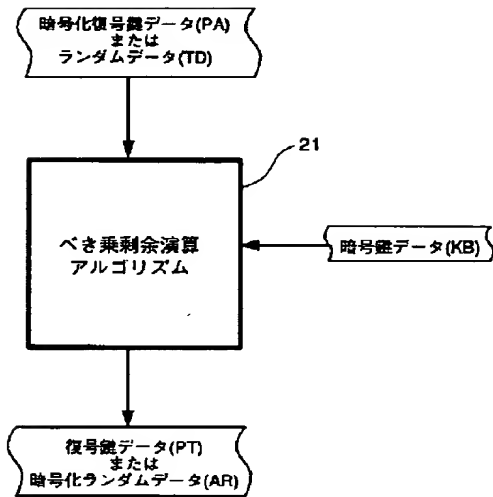


【図3】

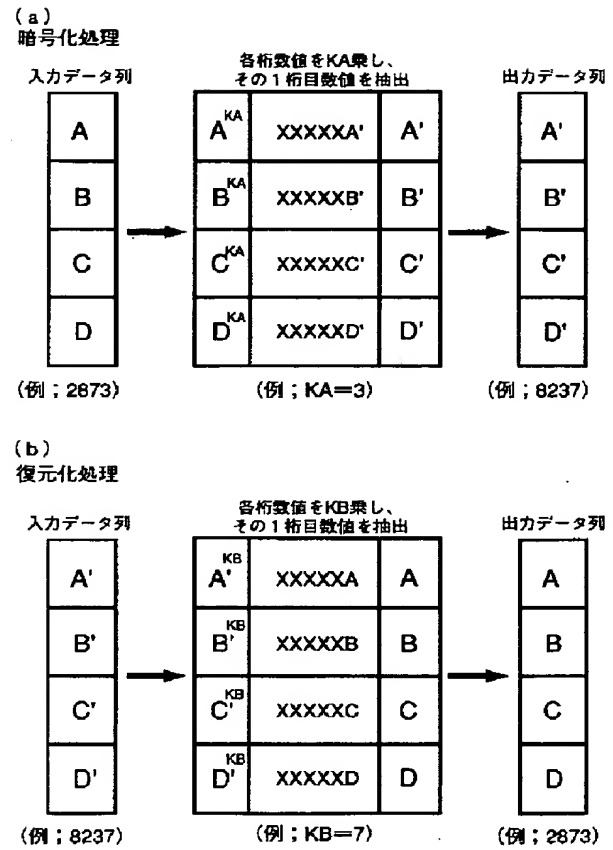




【図 4】



【図 5】



【図6】

